在RV34x系列路由器上配置Internet协议安全(IPSec)配置文件

目标

互联网协议安全(IPSec)在两个对等体（如两台路由器）之间提供安全隧道。应通过指定这些隧道的特征来定义被视为敏感且应通过这些安全隧道发送的数据包以及应用于保护这些敏感数据包的参数。然后，当IPsec对等体看到此类敏感数据包时，它会建立适当的安全隧道并通过此隧道将数据包发送到远程对等体。

当IPsec在防火墙或路由器中实施时，它可提供强大的安全性，可应用于跨边界的所有流量。公司或工作组内的流量不会产生与安全相关的处理开销。

本文档的目的是向您展示如何在RV34x系列路由器上配置IPSec配置文件。

适用设备

- RV34x系列

软件版本

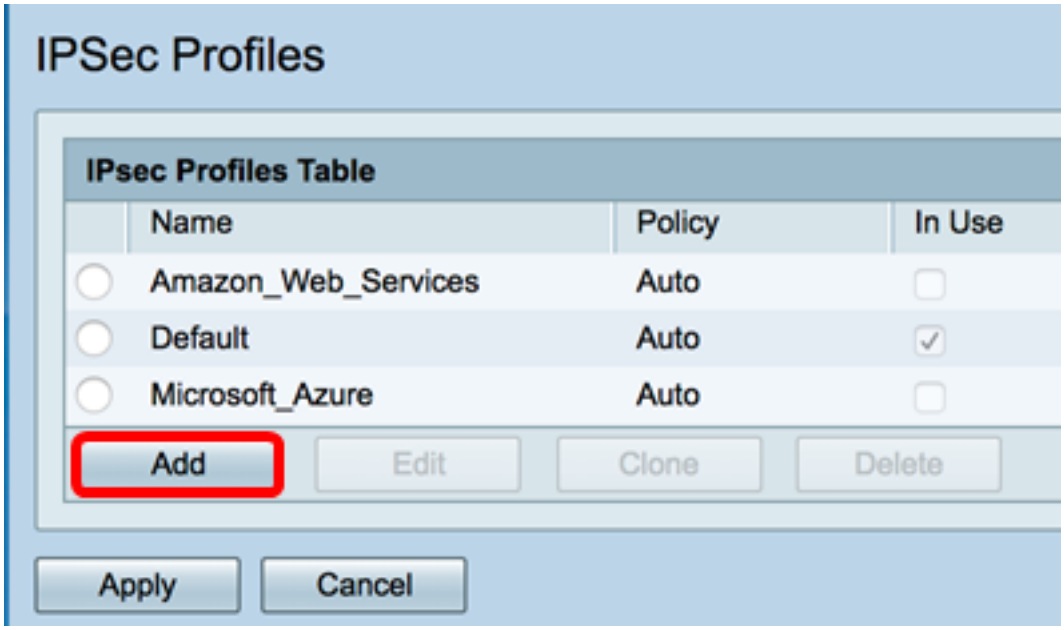
- 1.0.1.16

配置IPSec配置文件

创建IPSec配置文件

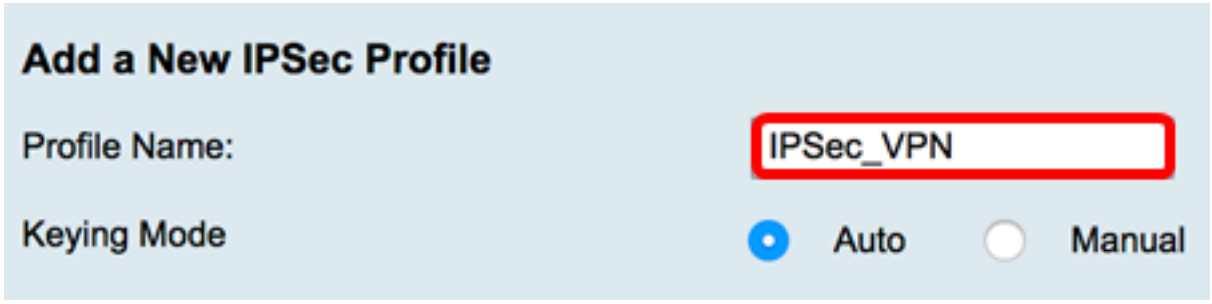
步骤1.登录到路由器的基于Web的实用程序，然后选择**VPN > IPSec Profiles**。

步骤2. IPsec配置文件表显示现有配置文件。单击**Add**创建新配置文件。



步骤3.在Profile Name字段中为配置文件*创建名*称。配置文件名称只能包含字母数字字符和特殊字符的下划线(_)。

注意：在本示例中，IPSec_VPN用作IPSec配置文件名称。



步骤4.单击单选按钮确定配置文件将用于验证的密钥交换方法。选项有：

- 自动 — 策略参数自动设置。此选项使用互联网密钥交换(IKE)策略实现数据完整性和加密密钥交换。如果选择此选项，则启用Auto Policy Parameters区域下的配置设置。单击此处以配置自动设置。
- 手动 — 此选项允许您手动配置用于虚拟专用网络(VPN)隧道的数据加密和完整性的密钥。如果选择此选项，则Manual Policy Parameters区域下的配置设置将启用。单击此处以配置手动设置。

注意：在本例中，选择了Auto。

配置自动设置

步骤1.在Phase 1 Options区域，从DH Group下拉列表中选择与Phase 1中的密钥一起使用的

适当Diffie-Hellman(DH)组。Diffie-Hellman是用于交换预共享密钥集的连接中使用的加密密钥交换协议。算法的强度由位决定。选项有：

- 组2 - 1024位 — 计算密钥的速度较慢，但比组1更安全。
- 组5 - 1536位 — 计算最慢的密钥，但是最安全。

注意：在本例中，选择Group2-1024位。

步骤2.从Encryption下拉列表中，选择适当的加密方法来加密和解密封装安全负载(ESP)和Internet安全关联和密钥管理协议(ISAKMP)。 选项有：

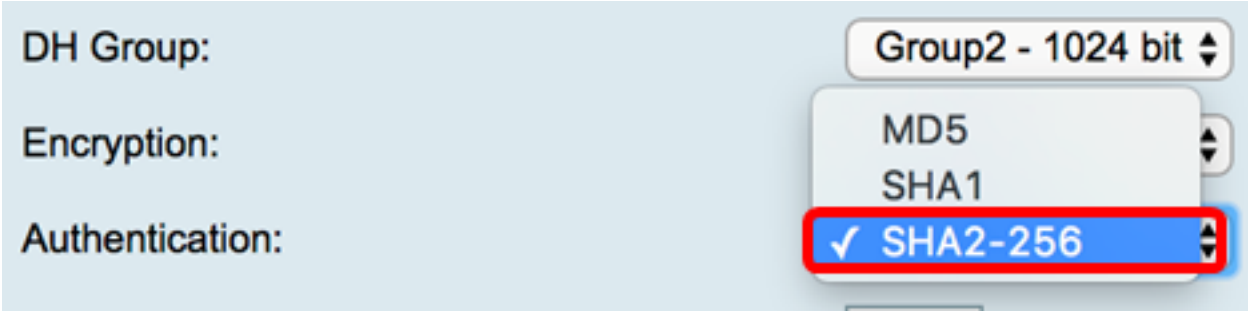
- 3DES — 三重数据加密标准。
- AES-128 — 高级加密标准使用128位密钥。
- AES-192 — 高级加密标准使用192位密钥。
- AES-256 — 高级加密标准使用256位密钥。

注意：AES是DES和3DES上的标准加密方法，因为它具有更高的性能和安全性。延长AES密钥将提高安全性，同时降低性能。在本例中，选择AES-256。

步骤3.从Authentication下拉菜单中，选择确定如何对ESP和ISAKMP进行身份验证的身份验证方法。选项有：

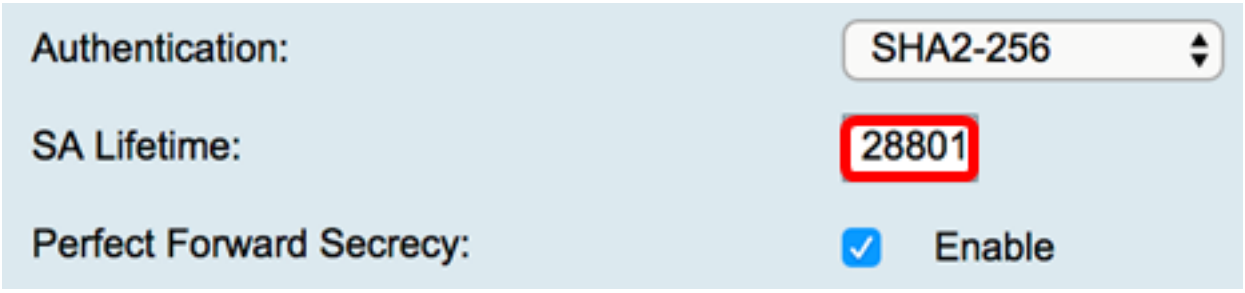
- MD5 — 消息摘要算法有128位哈希值。
- SHA-1 — 安全散列算法有160位散列值。
- SHA2-256 — 安全散列算法，带256位散列值。

注意：MD5和SHA都是加密哈希函数。他们提取一段数据，将其压缩，并创建一个通常无法重现的唯一十六进制输出。在本例中，选择SHA2-256。

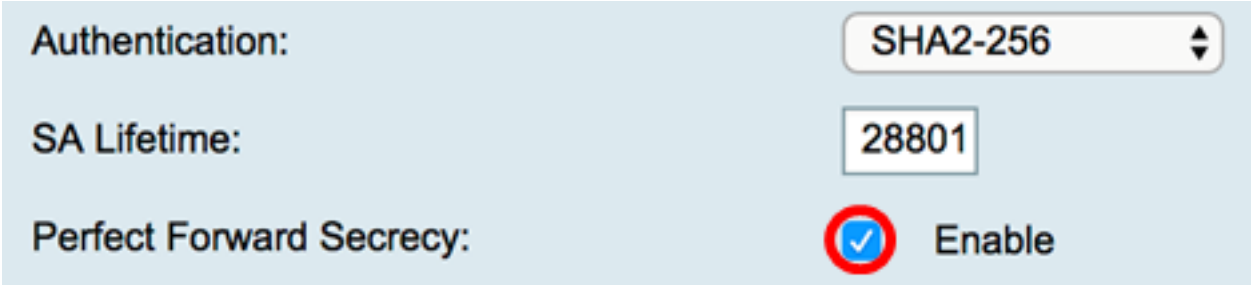


步骤4.在*SA Lifetime*字段中，输入介于120和86400之间的值。这是Internet密钥交换(IKE)安全关联(SA)在此阶段保持活动状态的时间长度。默认值为 28800。

注意：在本例中，使用28801。

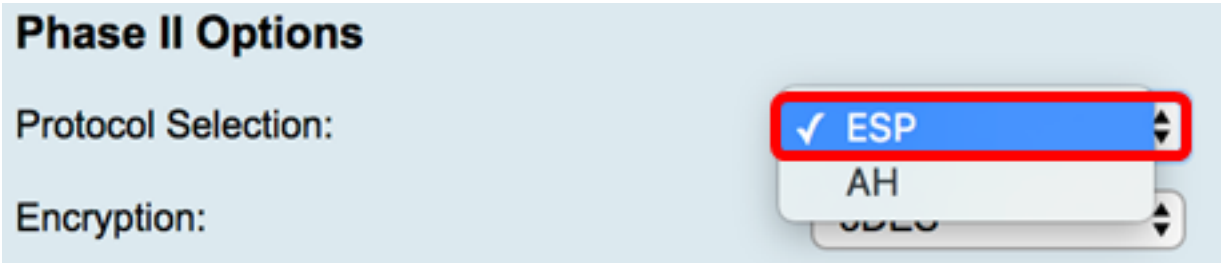


步骤5.（可选）选中**Enable Perfect Forward Secrecy复选框**，为IPSec流量加密和身份验证生成新密钥。



步骤6.从Phase II Options区域的Protocol Selection下拉菜单中，选择要应用于协商第二阶段的协议类型。选项有：

- ESP — 如果选择此选项，请跳至步骤7 ，以选择ESP数据包如何加密和解密的加密方法。一种安全协议，提供数据隐私服务、可选数据身份验证和反重播服务。ESP封装要保护的数据。
- AH — 身份验证报头(AH)是提供数据身份验证和可选防重播服务的安全协议。AH嵌入到要保护的数据（完整IP数据报）中。 如果选择了此选项，请跳至步骤8。

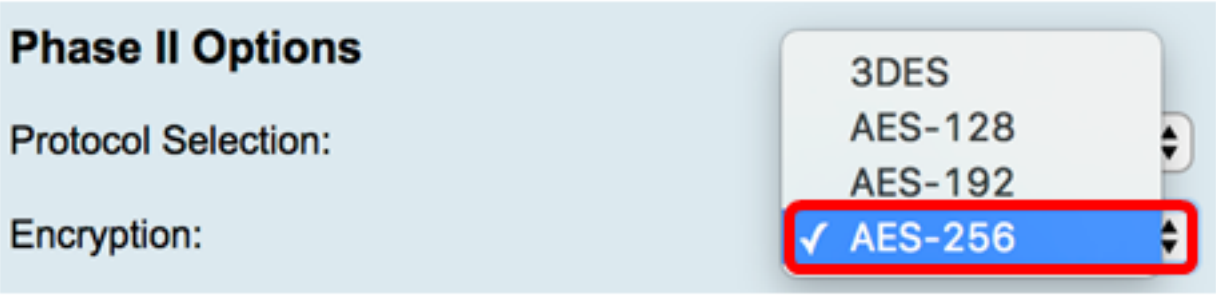


步骤7.如果在步骤6中选择了ESP，请从Encryption下拉列表中选择适当的加密方法来加密和解密ESP和ISAKMP。选项有：

- 3DES — 三重数据加密标准。
- AES-128 — 高级加密标准使用128位密钥。

- AES-192 — 高级加密标准使用192位密钥。
- AES-256 — 高级加密标准使用256位密钥。

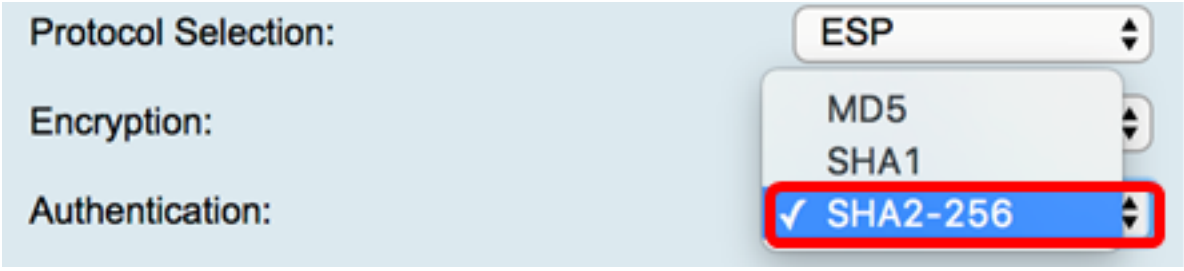
注意：在本例中，选择AES-256。



步骤8.从Authentication下拉菜单中，选择确定如何对ESP和ISAKMP进行身份验证的身份验证方法。选项有：

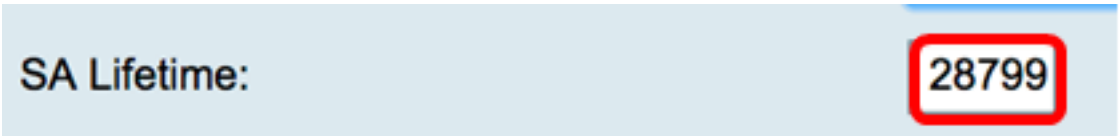
- MD5 — 消息摘要算法有128位哈希值。
- SHA-1 — 安全散列算法有160位散列值。
- SHA2-256 — 安全散列算法，带256位散列值。

注意：在本例中，使用SHA2-256。



步骤9.在*SA Lifetime*字段中，输入一个介于120和28800之间的值。这是IKE SA在此阶段保持活动状态的时间长度。默认值为 3600。

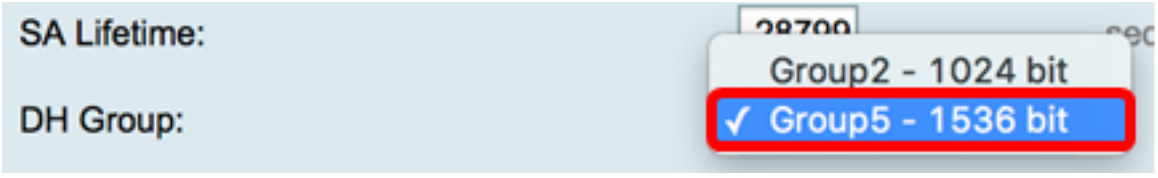
注意：在本例中，使用28799。



步骤10.从DH组下拉列表中，选择与第2阶段中的密钥一起使用的适当Diffie-Hellman(DH)组。选项包括：

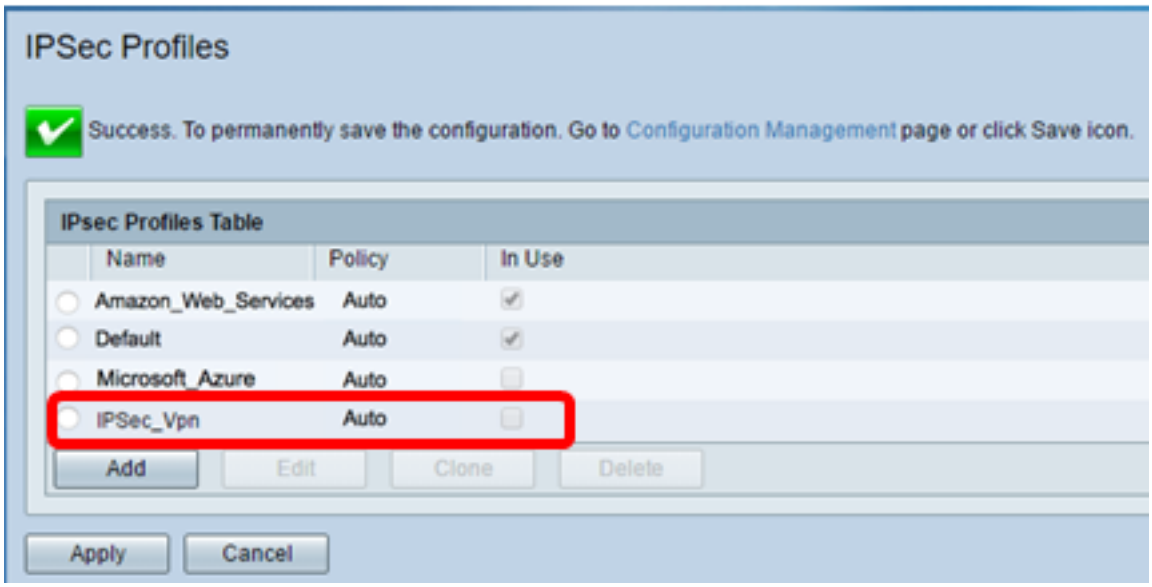
- 组2 - 1024位 — 计算密钥的速度较慢，但比组1更安全。
- 组5 - 1536位 — 计算最慢的密钥，但最安全。

注意：在本例中，选择组5 - 1536位。



步骤11.单击 Apply 。

注意：您将返回到IPSec配置文件表，此时应会显示新创建的IPSec配置文件。



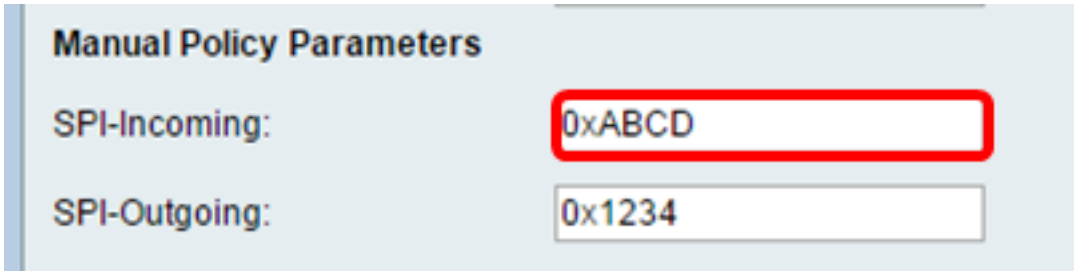
步骤12.（可选）要永久保存配置，请转至“复制/保存配置”页面，或单击页面上 Save 部分的图标。

现在，您应该已在RV34x系列路由器上成功配置了自动IPSec配置文件。

配置手动设置

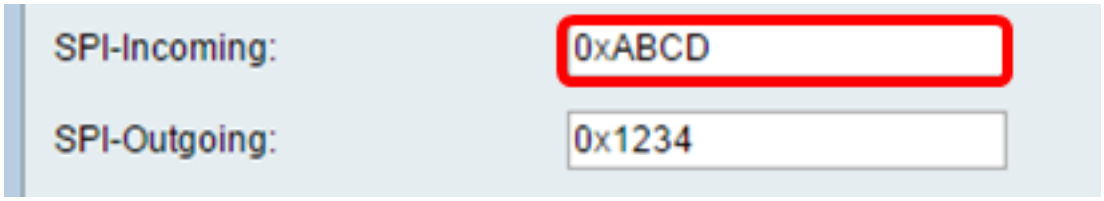
步骤1.在*SPI-Incoming*字段中，为VPN连接上的传入流量的安全参数索引(SPI)标记输入一个介于100到FFFFFFF之间的十六进制数。SPI标记用于区分一个会话的流量与其他会话的流量。

注意：在本例中，使用0xABCD。



步骤2.在*SPI-Outgoing*字段中，为VPN连接上的传出流量的SPI标记输入一个介于100到FFFFFFF之间的十六进制数。

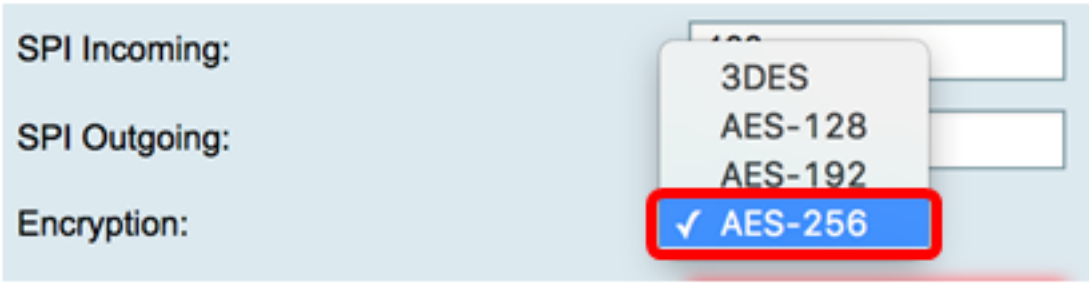
注意：在本例中，使用0x1234。



步骤3.从Encryption下拉列表中选择一个选项。选项为3DES、AES-128、AES-192和AES-

256。

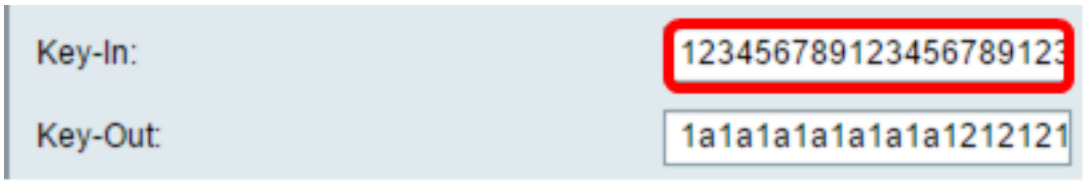
注意：在本例中，选择AES-256。



步骤4.在Key-In*字段中*，输入入站策略的密钥。密钥长度取决于步骤3中选择的算法。

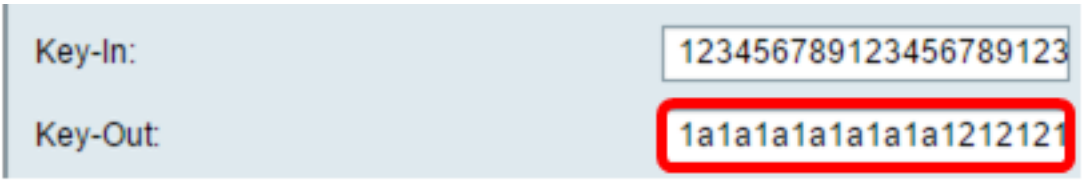
- 3DES使用48个字符的密钥。
- AES-128使用32个字符的密钥。
- AES-192使用48个字符的密钥。
- AES-256使用64个字符的密钥。

注意：在本例中，使用123456789123456789123...。



步骤5.在Key-*Out*字段中，输入传出策略的密钥。密钥长度取决于步骤3中选择的算法。

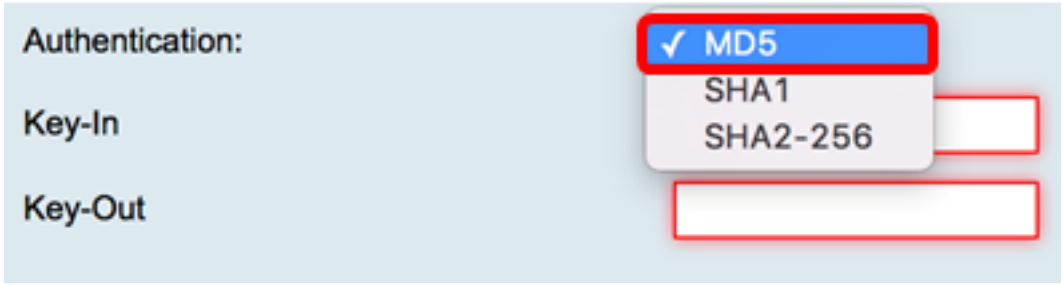
注意：在本示例中，使用1a1a1a1a1a1a121212...。



步骤6.从Manual Integrity Algorithm下拉列表中选择一个选项。

- MD5 — 使用128位哈希值实现数据完整性。MD5的安全性较低，但比SHA-1和SHA2-256快。
- SHA-1 — 使用160位哈希值实现数据完整性。SHA-1比MD5慢但更安全，而SHA-1比SHA2-256快但不安全。
- SHA2-256 — 使用256位哈希值实现数据完整性。SHA2-256比MD5和SHA-1慢但安全。

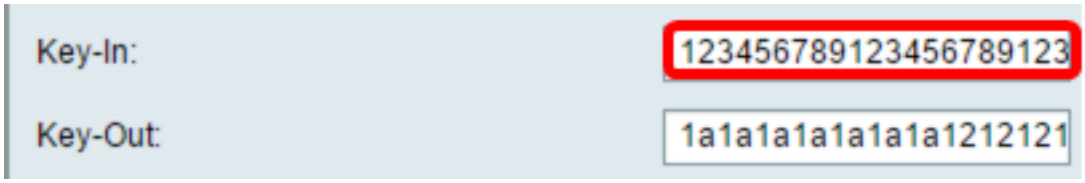
注意：在本例中，选择MD5。



步骤7.在Key-In*字段中*，输入入站策略的密钥。密钥长度取决于步骤6中选择的算法。

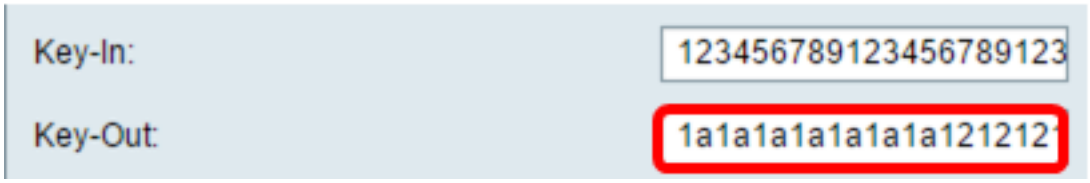
- MD5使用32个字符的密钥。
- SHA-1使用40个字符的密钥。
- SHA2-256使用64个字符的密钥。

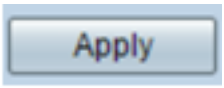
注意：在本例中，使用12345678912345678912 3...。



步骤8.在Key-*Out字段中*，输入传出策略的密钥。密钥长度取决于步骤6中选择的算法。

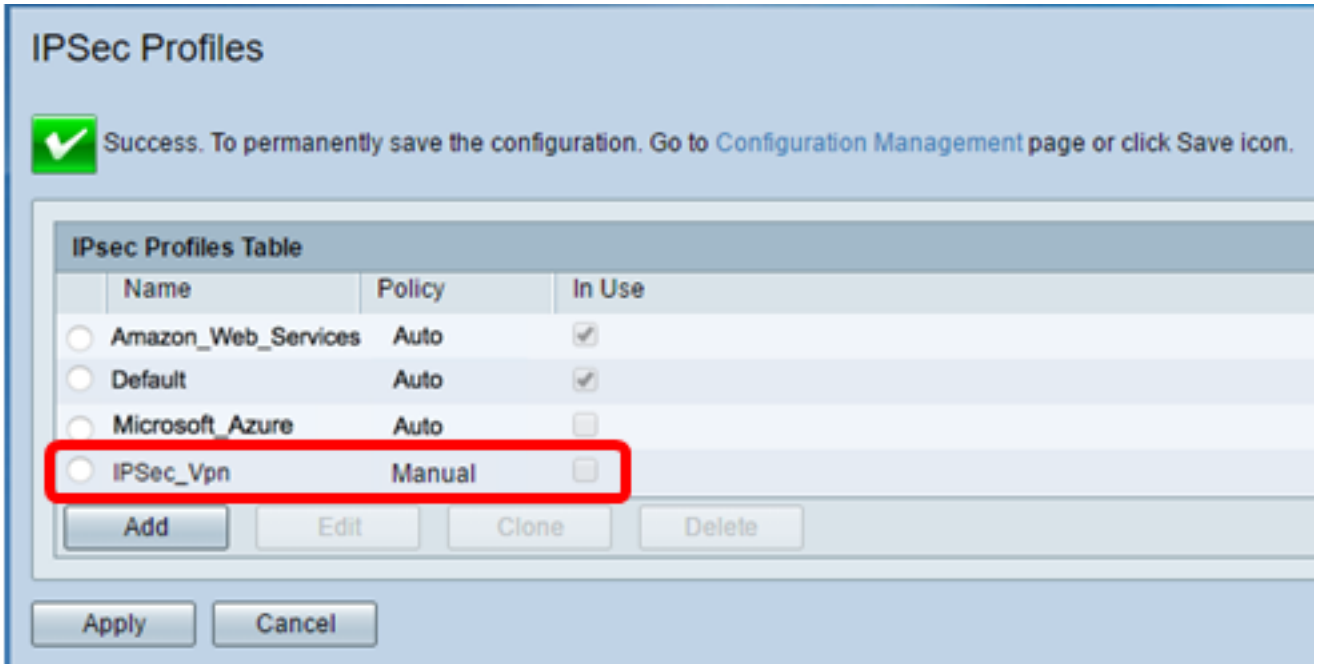
注意：在本示例中，使用1a1a1a1a1a1a121212...。



步骤9.单击 

。

注意：您将返回到IPSec配置文件表，此时应会显示新创建的IPSec配置文件。



第10步。（可选）要永久保存配置，请转到“复制/保存配置”页面，或单 

击页面上部的图标。

现在，您应该已在RV34x系列路由器上成功配置了手动IPSec配置文件。